AD-A057 522 BOEING VERTOL CO PHILADELPHIA PA F/G 6/7
SYSTEM SAFETY PROGRAM PLAN-EXTERNALLY MOUNTED, AUTOMATICALLY EX--ETC(U)
OCT 76 E W KING N62269-76-C-0341
UNCLASSIFIED D210-11138-1 NL

1 OF 1
ADA
057522

END
DATE
FILMED
9 -78
DDC

AD A057522

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

(2) LEVEL II

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER (14) D210-11138-1	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) (6) System Safety Program PLAN - Externally Mounted, Automatically Expelled/Inflated Multiplace Life Raft for Helicopters.		5. TYPE OF REPORT & PERIOD COVERED Final ((8) of (14)) Jun 1976 - Oct 1976
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) (10) E. W. King		8. CONTRACT OR GRANT NUMBER(s) (15) N62269-76-C-0341
9. PERFORMING ORGANIZATION NAME AND ADDRESS Boeing Vertol Company, Survivability Section P.O. Box 16858 Phila., PA 19142 (12) 26p.		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Prog. Element 63216N Proj. No. W0584001 Task Area No. W4567001 WU No. DS 903(Form DD1498)
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Air Development Center (6033) Aircraft & Crew Systems Technology Directorate Warminster, PA 18974		12. REPORT DATE (11) 4 Oct 1976
		13. NUMBER OF PAGES 24
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office) (16) W0584, W4567		15. SECURITY CLASS. (of this report) UNCLAS
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution unlimited

(9) Final rept. Jun-Oct 76,

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

(17) W0584001, W4567001

DDC RECEIVED AUG 16 1978 B

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Failsafe Design
Hazard Analysis
System Safety Program Plan
Automated Life Raft (ALR)
Airworthiness Qualification
Flight Evaluation Program

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document defines the Boeing-Vertol Division System Safety Program (SSPP) for the externally mounted, automatically expelled/inflated multiplace life raft for helicopters, (Automated Life Raft) (ALR) for the H-46 automated life raft program. Emphasis is placed on the system safety contribution to substantiation of the airworthiness characteristics of the automated life raft-equipped aircraft configuration. This plan provides for the evaluation of system hazards and implementation of the required hazard controls.

DD FORM 1473 1 JAN 73 EDITION OF 1 NOV 65 IS OBSOLETE S/N 0102-014-6601

403 682

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

Enclosure (1)
8-1162-2484

REV LTR

BOEING VERTOL COMPANY

A DIVISION OF THE BOEING COMPANY

P.O. BOX 16858
PHILADELPHIA, PENNSYLVANIA 19142

CODE IDENT. NO. 77272

NUMBER D210-11138-1

TITLE SYSTEM SAFETY PROGRAM PLAN-EXTERNALLY MOUNTED, AUTOMATICALLY EXPELLED/INFLATED MULTI PLACE LIFE RAFT FOR HELICOPTERS

ORIGINAL RELEASE DATE 12-30-76. FOR THE RELEASE DATE OF SUBSEQUENT REVISIONS, SEE THE REVISION SHEET. FOR LIMITATIONS IMPOSED ON THE DISTRIBUTION AND USE OF INFORMATION CONTAINED IN THIS DOCUMENT, SEE THE LIMITATIONS SHEET.

MODEL H-46 CONTRACT N62269-76-C-0341

ISSUE NO. ____ ISSUED TO: ____

PREPARED BY E W King / E. W. King DATE 9-21-76

APPROVED BY E Q / E. Quinn DATE 10/1/76

APPROVED BY G Windolph / G. W. Windolph DATE 10-4-76

APPROVED BY ____ DATE ____

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

78 07 31 041

FORM 46280 (5/73)

LIMITATIONS

ACCESSION for
NTIS White Section ☑
DDC Buff Section ☐
UNANNOUNCED ☐
JUSTIFICATION

BY
DISTRIBUTION/AVAILABILITY CODES

Dist.	AVAIL. and/or	SPECIAL
A		

This document is controlled by Product Assurance Group
Organization 7930

All revisions to this document shall be approved by the above noted organization prior to release.

ACTIVE SHEET RECORD

SHEET NUMBER	REV LTR	ADDED SHEETS SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR	ADDED SHEETS SHEET NUMBER	REV LTR	SHEET NUMBER	REV LTR
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											

FORM 46283 (7/67)

REVISIONS			
LTR	DESCRIPTION	DATE	APPROVAL

FORM 46282 (3/67)

ABSTRACT

This document defines the Boeing Vertol System Safety Program Plan (SSPP) for the "Externally Mounted, Automatically Expelled/ Inflated Multiplace Life Raft for Helicopters", (Automated Life Raft) (ALR) for the H-46 Automated Life Raft Program". Emphasis is placed on the System Safety Program contribution to substantiation of the airworthiness characteristics of the "Automated Life Raft Equipped Aircraft Configuration". This Plan provides for the evaluation of system hazards and implementation of the required hazard controls.

KEY WORDS

Failsafe Design
Hazard Analysis
Hazard Identification
Hazard Control
Airworthiness
System Safety Program
Automated Life Raft (ALR)
System Safety Program Plan
Airworthiness Qualification
Hazard Classification
Correction Action
Human Error
Flight Evaluation Program

TABLE OF CONTENTS

LIST OF FIGURES

1. SCOPE

The System Safety Program Plan (SSPP) defines the organization, controls, and tasks to achieve improvements in survival safety in the H-46 Helicopter through the addition of an Externally Mounted, Automatically Expelled/Inflated Multiplace Life Raft System, (Automated Life Raft) (ALR).

The System Safety Unit will accomplish tasks defined in this Plan, including definition of specific qualitative requirements which are translated into system safety design features. The SSPP follows the guidelines of MIL-STD-882. The plan is directed primarily towards the "Automated Life Raft System", however, the activities will also be directed towards definition of safety requirements for the total aircraft system to assure that the safety considerations for the "Automated Life Raft System" are kept in concert with the H-46 system safety objectives.

2. OBJECTIVE

The objective of the System Safety Program is to assure the identification, evaluation and correction of Automated Life Raft System hazards in a timely and effective manner. The objective shall be attained by ensuring that:

a. Hazards associated with the "Automated Life Raft System" components are identified, evaluated and eliminated or controlled to an acceptable level.

b. Control is established over hazards that cannot be eliminated by design selection to protect personnel, equipment and property.

c. Minimum risk is involved in the acceptance and use of new materials and new production and testing techniques.

d. Retrofit actions required to correct hazardous conditions are minimized through the timely inclusion of safety features.

e. The historical safety data generated by similar safety programs and operational experience shall be used to preclude the incorporation of previously identified hazards into the "Automated Life Raft System".

3. ORGANIZATION AND RESPONSIBILITY

The organization established to achieve the safety objective is shown in Figure 1. The Program Manager, H-46/107 Program, is responsible for designs that are compatable with the objectives of the H-46/107 Program.

The System Safety Unit of Product Assurance prepares the SSPP and, upon approval of the SSPP, has the direct responsibility for working, support and monitoring safety tasks.

a. Design Engineering

1. Preparation of subsystem/assembly block diagrams and functions in support of hazard analyses.
2. Preparation of data packages (drawings, schematics, design requirements) in support of design reviews.
3. Solutions to identified safety problems.

b. Technology Engineering

1. Determination of the effect of loss of function of a subsystem/component on aircraft operation in support of hazard analyses.
2. Solutions to identified safety problems.

c. Test Engineering

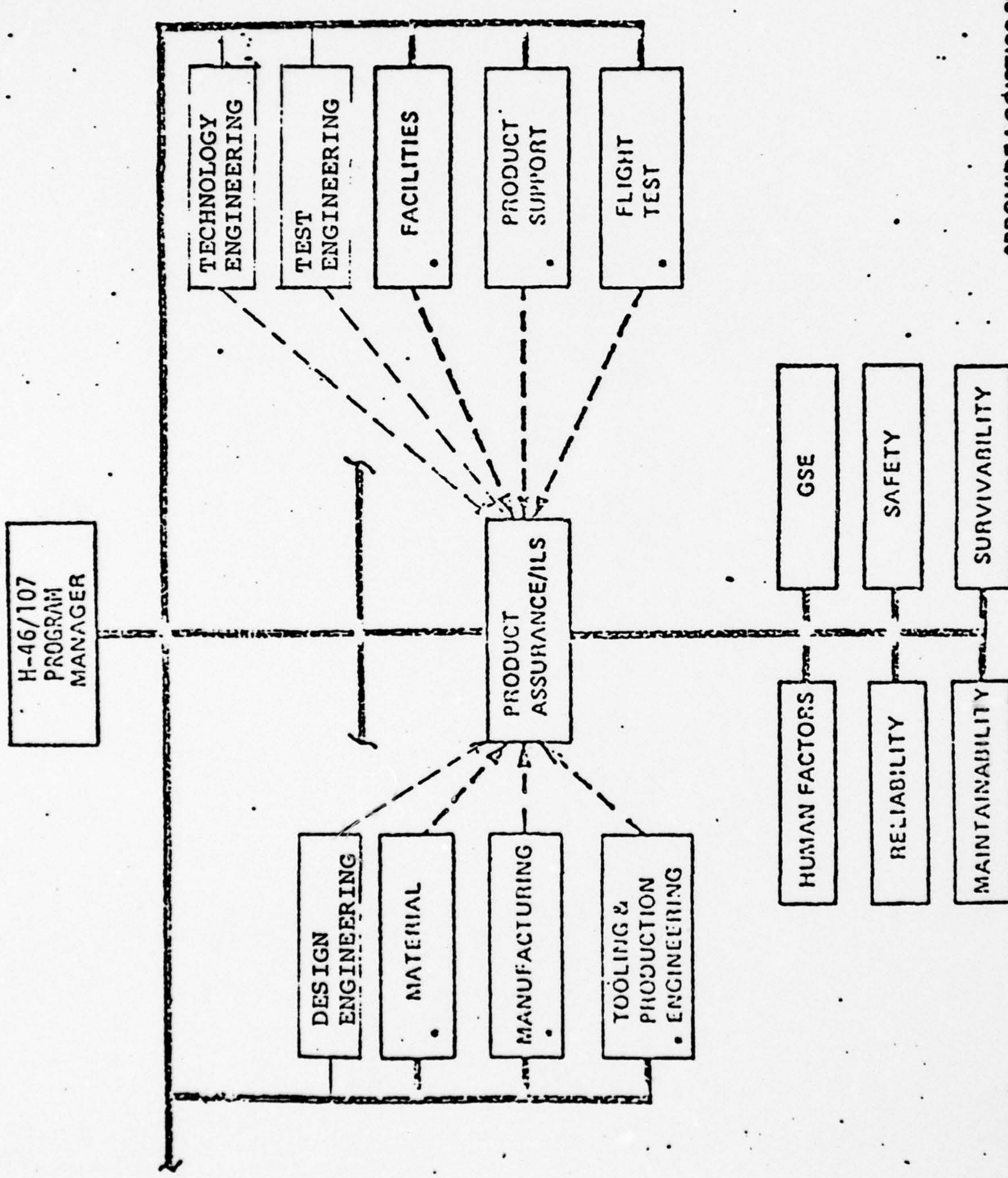
1. Preparation of test plans and procedures.
2. Reporting of malfunctions and failures.
3. Identification of test instrumentation interfaces with test subsystem/components in support of hazard analyses.

d. Human Factors Engineering

1. Identification of pilot/crew work tasks in support of hazard analyses.

e. Reliability Engineering

1. Material failure modes in support of hazards analyses.



•PROVIDE LOGISTICS SUPPORT

Figure 1 Organization Chart

3.1 INTERFACES

Probability of equipment malfunctions in support of hazards analyses.

a. Maintainability Engineering

Identification of maintenance tasks in support of hazards analyses.

b. Quality Assurance

Identification of hazard control procedures in support of making safety assessments.

c. Customer Technical Personnel

Formal and informal system safety reviews between contractor and customer safety personnel.

3.2 DESIGN SUPPORT

System safety design support is maintained through the implementation of a series of design reviews, trade reviews, and the establishment of a procedure for submitting safety recommendations/corrective actions.

3.3 SUBCONTRACTOR CONTROL

Safety control of products designed by Boeing and manufactured by others is exerted by normal quality control and inspection techniques. These techniques ensure that the safety designed into the product is not degraded by the subcontractor.

Safety control of products designed, fabricated, and tested by the subcontractor/supplier is exerted by the identification of design safety requirements in procurement specifications and specification control drawings. Subcontractors/suppliers are required to identify potential hazards that may exist in their design and describe corrective methods used to eliminate or control these hazards. Safety devices, warning systems, or compensating avoidance procedures will be described in those cases where the hazards cannot be eliminated. Subcontractors/supplier are required to:

a. Submit hazards analyses - These analyses must be approved by Boeing Vertol prior to design finalization.

b. Submit test plans which include provision for verification of safety requirements.

c. Participate in design reviews, as required by Boeing Vertol, to implement corrective action to remove or control potential hazards.

3.4 SYSTEM SAFETY PROGRAM ACTIVITIES

3.4.1 Requirements and Criteria

The primary task of establishing safety requirements and criteria is accomplished by (1) performing hazards analysis and (2) utilizing experience gained from other programs using similar systems and from the following experience retention sources:

a. Military Specifications
b. Contractual Documents
c. System Safety Design Handbook (AFSC DH1-6)
d. Vertol Design Instruction Manual (VDIM)
e. Mishap/Accident Analyses

These experience generated criteria are utilized by Preliminary Design Review participants and for inputs to design specifications.

3.4.2 Hazard Analyses

Hazard analyses will be performed to identify the hazardous elements or conditions in the air vehicle system and provide for their elimination or control. The following types of hazard analyses will be performed.

3.4.2.1 Subsystem Hazard Analyses (SSHA)

Subsystem Hazard Analyses will be performed to the level necessary to identify hazards for components and equipments whose performance degradation or functional failure could result in hazardous conditions. The SSHA uses the top-down approach. This approach is compatible with any level of design effort. Subsystem analysis starts when its functions are defined and detail functions are outlined. The following subsystem will be analyzed:

Externally Mounted, Automatically Expelled/Inflated, Multiplace Life Rafts For Helicopters

a. Life Rafts
b. Cool Gas Generators, Solid Propellent Generator

c. Life Raft Encapsulation
d. Harness and Retention System
e. Electrical Activation System

3.4.2.2 System Hazard Analysis (SHA)

Subsystem, Operational and Maintenance Hazard Analyses are generally limited in scope and may not bridge all the interfaces between subsystems, especially when redundancy is spread across two or more subsystems. In this respect the SHA is performed on the total system. The technique for performing the SHA considers the common causal factors as well as the spatial relationships between parts and subsystem.

3.4.2.3 Operating Hazard Analysis (OHA)

The Operating Hazard Analysis (OHA) will be performed to identify hazardous conditions related to the performance of tasks involving aircraft use. Control of operating hazards is generally attained by implementing appropriate procedures, instructions, and training. A flight profile will be defined (including operation in the intended environment of the H-46 Helicopter) from which the operating tasks will be derived. This analysis will be completed prior to first operations of the demonstration model.

3.4.2.4 Maintenance Hazard Analysis (MHA)

The Maintenance Hazard Analysis (MHA) is performed to identify hazards to the system which could result from faulty maintenance and to identify hazards which could cause injury to maintenance personnel. The MHA is conducted in conjunction with the maintenance tasks as defined by Maintainability Engineering. Control of these hazards may be in the form of procedures, cautions, training, or design changes.

3.4.2.5 The above analyses will consider the interfaces with GFE equipment, but not include detail analysis of GFE.

3.4.2.6 The above analyses will use, as practical, the data in the "Automated Life Raft Study" that was prepared under Contract N62269-75-C-0454.

3.4.3 Design Reviews/Trade Studies

The major design review effort by the safety engineer occurs "over the drawing boards" and in informal design reviews. Conclusions reached during hazards analyses and experience retention analyses are made available to design review participants. The safety engineer also participates in design trade studies.

3.4.4 Corrective Action Procedure

The corrective action procedure for identified safety problems is described below.

3.4.4.1 Hazard Categorization and Evaluation

The Hazard Categorization and Evaluation Cycle is illustrated by Figure 2. Hazards will be classified on the basis of worse potential consequences which could ultimately occur if the hazard is not eliminated.

These classifications will never change unless the original predicted consequence requires revision or the classification selected is in error. The hazard cause factors will include personnel error, environmental conditions, system design characteristics, procedural deficiencies, and material failure or malfunction. Classification of the consequence or effect of hazards will be expressed in terms of the severity of their effects on personnel and the material.

a. Class I - Negligible

   1. The consequences of the condition will not result in personal injury or system damage.

b. Class II - Marginal

   1. The consequences of the condition can be counteracted or controlled without injury to personnel or major system damage.

c. Class III - Critical

   1. The consequences of the condition will cause personnel injury or major system damage, or will require immediate corrective action for personnel or system survival.

d. Class IV - Catastrophic

   1. The consequences of the condition will cause death or severe injury of personnel or system loss.

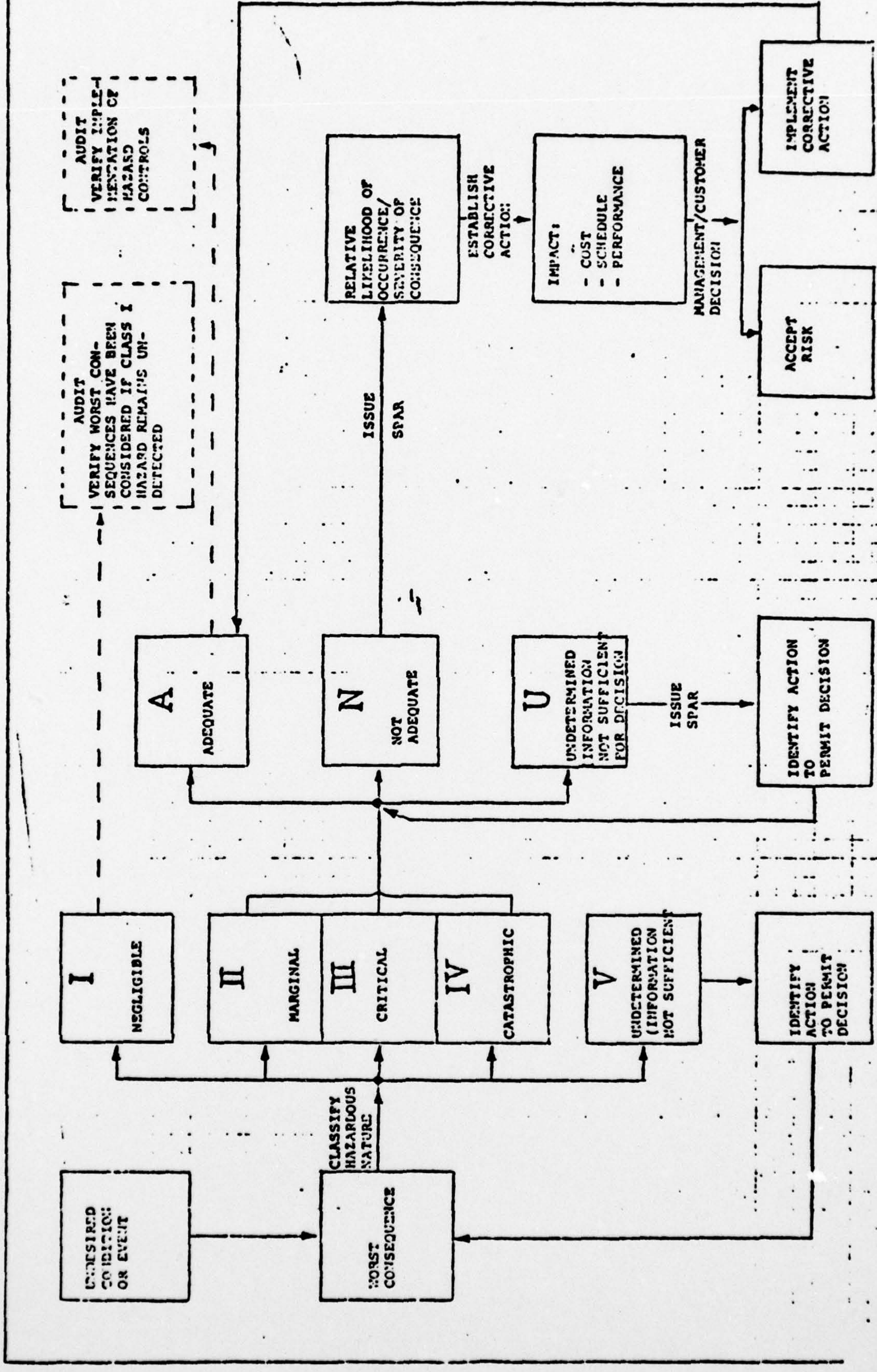


FIGURE 2 - Hazard Categorization and Evaluation Cycle

e. Class V - Undetermined

1. The consequences of the condition cannot be determined at this time. Additional technology, analysis, or test are required to substantiate the effects on the system.

A safety assessment will be made for those hazards which cannot be eliminated. The assessment shall be indicated as follows:

"A" - Adequate - The occurrence of the hazard is considered to be unlikely with the controls provided.

"B" - Not Adequate - The occurrence of the hazard is considered to be likely, and controls are not considered sufficient or do not exist.

Hazards that have been designated with a safety assessment of "Not Adequate" or "Undetermined" will be documented on a Safety Problem Action Report (SPAR) as described in Paragraph 3.4.4.2.

The above process effectively prioritizes identified hazards and directs attention to those areas requiring further investigation and management decision for corrective action. Resources required to establish corrective action will be identified when the program costs, schedule, or system performance are significantly affected.

3.4.4.2 Action on Identified Hazards

A closed loop procedure will be used for tracking action status of identified safety problems (hazardous conditions). Sources of problem identification include hazard analyses, design reviews, test experience, and mishap data available from the Armed Services Safety Agencies.

Safety problems will be documented on a Safety Problem Action Report (SPAR) Form (see Figure 3). SPAR's will be closed out after implementation of the required corrective action has been verified. Each SPAR will be chronologically numbered and cross-referenced to appropriate subject categories selected from the Work Breakdown Structure (WBS).

The System Safety Engineer will identify the problem with appropriate recommendations and coordinate problem investigation with the cognizant design, technology and/or test engineer. The required action is recorded and the Safety Engineer and the Design, Technology or Test Engineer sign the SPAR as approval of the corrective action.

Status of SPAR's will be reported in the Safety Statement.

TO:	SAFETY PROBLEM ACTION REPORT	
SUBJECT:	PROGRAM: ______	SPAR NO.: ______
	ORIGINATOR: ______	DATE: ______

PROBLEM:

EXISTING CONTROLS:

ASSESSMENT/RECOMMENDATIONS:

CORRECTIVE ACTION: DATE:

CORRECTIVE ACTION APPROVAL	DESIGN PROJECT ENGINEER DATE:	SYSTEM SAFETY ENGINEER DATE:

FIGURE 2 SAFETY PROBLEM ACTION REPORT FORM

3.4.5 Program Review

System Safety Program Informal Reviews will be scheduled as required. The Contractor will be prepared to discuss or answer questions relative to safety activities as defined by Safety Statements or other safety related agenda items as approved by the Navy Program Manager.

3.4.6 Test Requirements and Reviews

3.4.6.1 Test Plans

Safety Engineers will review test plans and recommend safety requirements as appropriate. These requirements will be generated from hazard analyses and/or experience retention data. Test results will be reviewed for compliance with the test requirements.

3.4.6.2 Failure/Malfunction Reporting

Equipment failure/malfunctions for all test phases (bench testing, demonstration, test rig, flight testing) will be reported to Safety Engineering so that these "potential hazards" may be included in hazard analyses and their effect determined on aircraft operation. Test Engineering has the responsibility to report such failures/malfunctions to the Safety Engineering Group.

3.4.6.3 Flight Test Accident/Incidents

The procedure for investigation and reporting an aircraft accident/incident will follow the guidelines of Boeing Vertol Operating Procedure 700.49, "Aircraft Accident or Incident Investigation."

3.4.7 Safety Statements

Safety Statements will be prepared in accordance with the format shown by Figure 4, and will be submitted as required.

4. SYSTEM SAFETY ACTIVITIES AND MILESTONE SCHEDULE

System safety activities and milestone schedules will be in accordance with Figure 5.

HELICOPTER FLOTATION SYSTEM SAFETY STATEMENT

1. Table of Contents

List of each subsystem and its page number.

2. Introduction

Summarize all actions completed or initiated during reporting period. Provide a narrative on status of overall safety program.

3. Subsystems

List each subsystem separately and present the following for each subsystem.

a. Description - Describe the subsystem, identifying the components within the subsystem and their sequence of operation. Schematic diagrams shall be included for each major subsystem to aid in the understanding of the relationships between components. The interfaces of the subsystem with other subsystems shall be included in the discussion and schematics.

b. Hazards - Any potential hazards identified during the particular reporting period for the Safety Statement or any hazards identified, but not eliminated or controlled in previous Safety Statements shall be presented in this section. The hazards will be referenced by their tracking system designation. Possible alternatives of corrective action will be presented for all identified hazards. The Contractor shall select the most feasible form of corrective action as early in the design phase as possible and present his reasons for the selection of this particular alternative.

4. Failure Mode Analysis

Summarize any quantitative/qualitative analyses, and present any test results performed to support information contained in the Safety Statement.

5. References

List all pertinent references.

FIGURE 4 - General Format for Safety Statement

LEGEND

SYSTEM SAFETY
PROGRAM MILESTONES

BOEING V. ,OL COMPANY

SYSTEM SAFETY PROGRAM PLAN-EXTERNALLY MOUNTED, AUTOMATICALLY EXPELLED/INFLATED MULTIPLACE LIFE RAFT FOR HELICOPTERS

SCHEDULING DATA SHEET

PROGRAM ______

CONTRACT ______

AUTHORIZATION ______

ISSUED BY ______
CODE NO. ______
DATE ISSUED ______
DATE REVISED ______
PREPARED BY ______
APPROVED ______
APPROVED ______

ACTIVITY

Months: 1 2 3 4 5 6 7 8 9 10 11 12 | 1 2 3 4 5 6 7 8 9 10 11 12 | 1 2 3 4 5 6

PHASE III

PHASE IV DEMONSTRATION

PHASE V PROTOTYPE DEVELOPMENT AND TESTING

PHASE VI PRODUCTION DEVELOPMENT

- SSSP APPROVED
- UPDATE PRELIMINARY HAZARDS ANALYSIS
- SSHA REPORTS
- MHA REPORTS
- OHA REPORTS
- SHA REPORTS
- SAFETY STATEMENTS
- DESIGN REVIEWS
- COMPONENT DELIVERIES
- COMPONENT ASSEMBLY AND TEST
- SUB ASSEMBLY DEMONSTRATION
- DEMONSTRATION MODEL REVIEW
- WIND TUNNEL TESTING
- PROTOTYPE TESTING
- FINAL SAFETY STATEMENT

THIS PAGE IS BEST QUALITY PRACTICABLE
FROM COPY FURNISHED TO DDC

FORM 22-60 (3/73)

FIGURE 5

5. DOCUMENTATION

The SSPP shall be updated, as required.

The contractor will submit Safety Statements to the procuring agency, as required.

All other system safety data will be available in the Contractor's file for government review.

6. AIRWORTHINESS SUBSTANTIATION

The following activities of the "Automated Life Raft" SSPP will form the system safety portion of the Airworthiness Qualification Program.

a. Review of hazard analyses.

b. Safety Problem Action Report (SPAR) status.

c. Compliance with model specification and contract safety requirements.

d. Review of test and demonstration plans.

e. Review of test results.

f. Review of interim safety statements.

7. U.S. NAVY EVALUATION TESTS

The system safety activities in support of U.S. Navy Evaluation Tests will include:

a. Update of the final safety statement submitted to the government 30 days after completion of Demonstration Model Testing.

8. SAFETY ACTIVITIES

8.1 SAFETY DATA

The safety data provided by the Naval Aviation Safety Center, Norfolk, VA was utilized in the preparation and evaluation of the safety analyses.

8.2 TRAINING

The Contractor shall develop and conduct an in-house training program to qualify and develop capabilities of System Safety organization personnel in the hazard analyses techniques and other tasks specified in the SSPP. System Safety shall review instruction plans and materials to be used in the training of flight, maintenance and test personnel for inclusion of appropriate safety information.

8.3 AUDIT PROGRAM

An audit shall be accomplished to verfiy implementation of actions designated to control all identified hazards. The audit will consist of a review of production drawings, functional test procedures, operating, and maintenance instructions by the System Safety Group. Results of the audit will be included in the Safety Statements.

8.4 GROUND HANDLING, STORAGE, SERVICING AND TRANSPORTATION

The System Safety Program shall be applicable to all phases of System Ground Handling.

Hazards analyses shall include hazards encountered during these ground operations.

Life Raft System Equipment will be handled, stored, serviced and transported in accordance with established survival equipment requirements.

8.5 SAFETY TESTING

Safety Testing is integrated into appropriate test plans. The tests will be performed on critical components to determine the category of hazard and/or the margin of safety present in the design. The System Safety Input is derived from the Operating Hazard Analysis (OHA).

The detail test plans will be structured to assure that testing is carried out in a safe manner and that hazards introduced by testing procedures, instrumentation, or test hardware are identified and minimized.

9. SUB CONTRACTOR/VENDOR/SUPPLIER SYSTEM SAFETY PROGRAM APPLICABILITY

The requirements of this plan apply to program participants where necessary in order to achieve SSSP objectives.

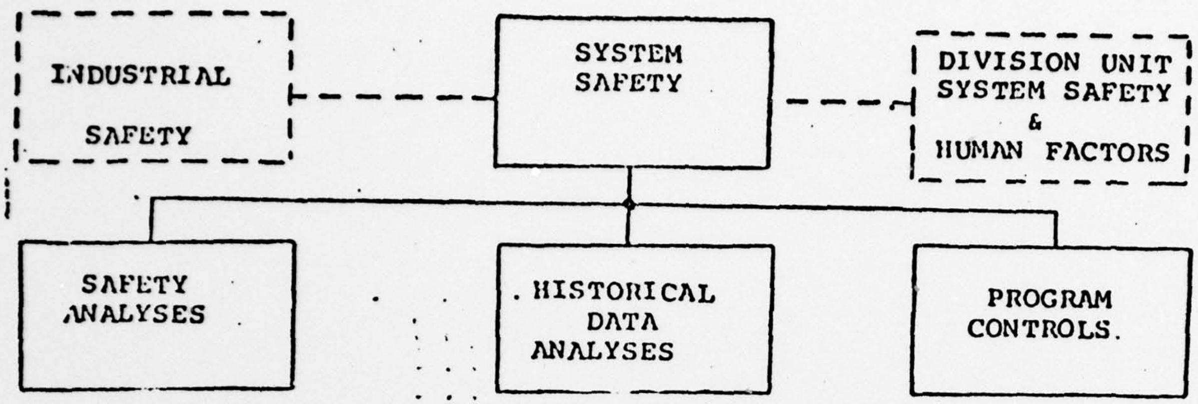
Subcontractors, vendors and suppliers will perform analyses as necessary to identify hazards and describe corrective methods used to control or eliminate such hazards as related to their specific products.

10. EXPLOSIVES AND ORDINANCE

Not Applicable.

11. SYSTEM INSTALLATION

Figure 6 illustrates the management structure from which will be provided on the job safety surveillance during system installation, checkout and modification activities.



- Safety Criteria
- Design Review & Assessment
- Preliminary Hazard Analyses
- System Hazard Analysis
- Subsystem Hazard Analyses
- Maintenance Hazard Anal.
- Operational Hazard Analyses
- Safety Problem Action Report (SPAR)
- SPAR Corrective Action Audit
- Test Results Review

- Accident Data Review
- Subsystem Failure Data
- Accident Trend Analyses

- System Safety
- Requirements Integration
- Procurement Specifications
- Hazard Analysis Reports
- SSP Review Meeting
- Safety Statements
- Drawing Sign-off

FIGURE-6 . SYSTEM SAFETY UNIT MANAGEMENT STRUCTURE